MONITORAMENTO E SEGURANÇA DE DADOS

BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Para iniciar esse assunto segue alguns dados apresentados de pesquisas sobre segurança cibernética realizado pelo site Cybersecurity Ventures.

Os danos por crimes cibernéticos custarão ao mundo US $ 6 trilhões anualmente até 2021.

Isso representa a maior transferência de riqueza econômica da história, arrisca os incentivos à inovação e ao investimento e será mais lucrativo do que o comércio global de todas as principais drogas ilegais juntas.

Os custos de crimes cibernéticos incluem danos e destruição de dados, dinheiro roubado, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, peculato, fraude, interrupção pós-ataque ao curso normal dos negócios, investigação forense, restauração e exclusão de hackers dados e sistemas e danos à reputação.

Prevê-se que os custos globais de danos ao ransomware atinjam US $ 20 bilhões até 2021.

Os ataques de ransomware a organizações de assistência à saúde - muitas vezes chamados de indústria número 1 de ataques cibernéticos - quadruplicarão até final de 2020.

A Cybersecurity Ventures espera que uma empresa seja vítima de um ataque de ransomware a cada 11 segundos até 2021, em comparação a cada 14 segundos em 2019. Isso faz do ransomware o tipo de crime cibernético que mais cresce.

Para evitar que esses dados aumentem, descrevemos a seguir algumas práticas que ajudam a se prevenir desses possíveis ataques:

1. Sempre desconfiar de emails não solicitados

Atualmente, uma das principais formas dos cibercriminosos agirem é por meio de ataques phishing que contaminam os emails recebidos pelos usuários. Portanto, antes de abrir qualquer mensagem, é importante refletir "*Eu solicitei algum serviço deste remetente*?". É muito comum hackers se passarem por bancos ou outras instituições mandando cobranças, boletos, multas e afins. Por isso, é necessário identificar se a mensagem é verdadeira ou não e, assim, não abrir o email, eliminando a ameaça.

2. Verificar os remetentes

Muitos emails recebidos parecem ser verídicos e direcionado para os usuários. Isso porque o cibercrime está cada dia mais inovador à medida que utilizam tecnologias modernas, como a Inteligência Artificial a seu favor. Por isso, uma das primeiras coisas a serem feitas ao receber um email é verificar o remetente. O usuário estava esperando por aquele email? Conhece a pessoa que está enviando? É necessário verificar se o endereço de email está correto, pois muitas vezes os hackers se passam por empresas conhecidas, mas trocam algumas letras no nome. Este é o primeiro alerta que é falso, portanto, jogue-o na lixeira rapidamente.

3. Nunca abra anexos de desconhecidos

Só depois de analisar todas as informações sobre o remetente, é que você deverá abrir qualquer anexo enviado por e-mail, entretanto, vale a pena uma atenção maior com algumas extensões como .exe, .bat, .rar e .zip, pois são arquivos que podem possuir comandos executáveis de arquivos maliciosos.

4 Nunca disponibilizar logins e senhas, mesmo que para colegas de trabalho.

Se você fornece seus dados pessoais para alguém você precisa ter em mente que esta pessoa poderá utilizar esses dados para quaisquer ações. Sendo assim, caso ele(a) utilize-os a fim de roubar informações, danificar sistemas ou cometer infrações, você não terá como provar que não foi o infrator. Além disso, nem todos trabalham com acesso às mesmas informações, o que quer dizer que talvez você possua informações que são confidenciais e que não devem ser compartilhadas com outros membros da empresa.

5. Checar o domínio em sites

Assim como nos emails, muitos sites maliciosos possuem o mesmo layout dos verdadeiros, com apenas algum detalhe diferente. Com isso, acabam conseguindo facilmente enganar os usuários. Portanto, antes de acessá-lo e preencher qualquer informação pessoal nele, é necessário verificar seu domínio. É importante pesquisar na internet sobre aquele site, caso seja malicioso, outras pessoas podem estar comentando sobre ele e emitindo alertas.

6. Utilizar as redes sociais com segurança, não disponibilizando informações sigilosas ou fazendo contato com desconhecidos.

Hoje em dia, cibercriminosos utilizam as redes sociais para coletarem informações relevantes, como ocupação, endereço, amigos e gostos, sobre seus alvos a fim de usá-las em ataques de engenharia social.

7. Cuidado com downloads

Baixar arquivos, programas ou fontes (no caso dos designers, publicitários e videomakers) é algo corriqueiro na vida online, independente da área de atuação, mas é preciso atenção na hora de escolher os sites e fontes para fazer o download. Um arquivo mal-intencionado pode destruir a sua máquina, apagar todas as informações e causar prejuízos irremediáveis, a contar pelos dados presentes ali. Portanto, verifique a procedência do site e, ao receber qualquer aviso do antivírus, não continue com o download.

8. Nunca fotografar o ambiente de trabalho, principalmente telas de computador e documentos.

Suponha que você fotografou alguns documentos e gráficos da empresa para poder trabalhar de casa. Mas, acontece que você não sabia que seu telefone celular estava infectado com um malware, que permitia que um grupo de ciberatacantes tivesse acesso a todos os dados do seu celular. Sendo assim, à medida que você disponibilizou informações sobre a empresa no seu dispositivo, os cibercriminosos tiveram acesso a esses dados, expondo sua empresa, ou seja, deixando-a vulnerável apenas por um comportamento negligente seu.

9.Acesse redes wi-fi seguras

Evite as redes públicas de Wi-Fi, desconhecidas ou compartilhadas. Restaurantes, cafés e condomínios podem oferecer esse benefício aos seus clientes, porém esse serviço pode oferecer “brechas” de segurança que facilmente são alvos de ataques de cibercriminosos. Isso porque as redes públicas não possuem ferramentas de proteção padrão adequadas que garantam a proteção de dados pessoais como protocolos de segurança, firewall, criptografia entre outras. Além disso, evite também compartilhar sua senha e usuário com vizinhos de prédio ou condomínio. Isso pode expor seus dados e sobrecarregar seu sistema.

10. Chamar a TI quando necessário

Mesmo tomando todos os cuidados possíveis, os usuários ainda podem cometer erros e suspeitar de que alguma ameaça está afetando seus dispositivos. Nesses momentos, é crucial avisar a equipe de TI o mais rápido possível. Quando os profissionais certos sabem sobre o problema ainda no início, as chances de prejuízos são menores. Assim, podem tomar as medidas necessárias para eliminar a ameaça.

Fontes: https://blogbrasil.comstor.com/6-dicas-praticas-de-seguranca-da-informacao-para-usuarios
https://cartilha.cert.br/
https://blog.diferencialti.com.br/seguranca-da-informacao-praticas-para-usuarios/
https://www.proof.com.br/blog/conscientizacao-de-usuarios-seguranca-da-informacao/
https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/

TOOR.
MONITORAMENTO E SEGURANÇA DE DADOS

41 3526-0710